Wykrywanie i reagowanie na zagrożenia. Od alertu do realnej odporności organizacji



Firma Integrity Partners, NIP: 5272620067 / KRS: 0000347184 (dalej Partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanych dalej „Materiałami"), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich.

Spis treści

Wstęp 3

Dlaczego klasyczna ochrona już nie wystarcza 3

Wykrywanie zagrożeń na różnych poziomach 4

EDR (*ang. Endpoint Detection and Response*) – perspektywa punktu końcowego ... 4

NDR (*ang. Network Detection and Response*) – perspektywa sieci 4

XDR (*ang. Extended Detection and Response*) – szerszy kontekst incydentu 4

SIEM (*ang. Security Information and Event Management*) – centralna warstwa analityczna 5

SOAR (*ang. Security Orchestration, Automation and Response*) – koordynacja reakcji 5

Cloud Security / CNAPP (*ang. Cloud-Native Application Protection Platform*) – perspektywa środowisk chmurowych 5

Od alertu do reakcji 5

SOC, czyli zespół, który zamienia alerty w reakcję 6

Tożsamość jako nowy bastion cyberbezpieczeństwa 7

Rola AI w detekcji, reakcji i nowych ryzykach 8

Rola kompetentnego zespołu w budowie architektury odporności 8

Podsumowanie 9

Wstęp

Współczesne cyberbezpieczeństwo nie kończy się na ochronie przed atakiem. Kluczowe jest to, jak szybko organizacja potrafi wykryć zagrożenie, zrozumieć jego kontekst i zareagować, zanim incydent wpłynie na dane, użytkowników lub ciągłość działania biznesu. Dlatego skuteczny model Detection & Response powinien łączyć monitoring sieci, punktów kocowych, chmury, aplikacji i tożsamości z procedurami reakcji oraz wsparciem kompetentnego zespołu ekspertów.

Krajobraz cyberzagrożeń stale się zmienia. Dziś organizacje mierzą się z ukierunkowanymi, wieloetapowymi atakami ransomware, operacjami typu APT (*ang. Advanced Persistent Threats*), kampaniami phishingowymi wspieranymi przez generatywną sztuczną inteligencję oraz atakami wymierzonymi w tożsamość użytkowników, konta uprzywilejowane i systemy chmurowe.

Dlaczego klasyczna ochrona już nie wystarcza

W tym środowisku granice tradycyjnej sieci korporacyjnej uległy rozmyciu. Praca hybrydowa, migracja do chmury, aplikacje SaaS (*ang. Software as a Service*), API (*ang. Application Programming Interface*), urządzenia mobilne oraz integracja systemów IT z infrastrukturą przemysłową OT (*ang. Operational Technology*) sprawiły, że klasyczny model ochrony przestał wystarczać. Organizacja potrzebuje modelu bezpieczeństwa, który obejmuje wiele warstw jednocześnie i pozwala reagować tam, gdzie faktycznie pojawia się zagrożenie.

Wykrywanie i reagowanie na cyberzagrożenia to proces wielowarstwowy. Wymaga połączenia technologii, procedur, automatyzacji oraz wiedzy ekspertów. Jego celem nie jest wyłącznie wygenerowanie alertu, ale szybkie ustalenie, co się wydarzyło, jakiego zasobu dotyczy incydent, jaki jest jego wpływ na organizację i jakie działania należy podjąć. Dobrze zaprojektowany model wykrywania i reagowania zwiększa odporność organizacji, skraca czas reakcji oraz ogranicza ryzyko przestojów, utraty danych i eskalacji incydentu.

Znaczenie tego podejścia rośnie również w kontekście regulacyjnym. Dyrektywa NIS2 (*ang. Network and Information Security Directive 2*), rozporządzenie DORA (*ang. Digital Operational Resilience Act*) oraz inne wymagania dotyczące cyberodporności wzmacniają potrzebę stałego monitorowania środowiska, dokumentowania incydentów, kontroli dostępu i gotowości do szybkiej reakcji.

Wykrywanie zagrożeń na różnych poziomach

Skuteczna obrona przed cyberatakami wymaga monitorowania stanu cyberbezpieczeństwa z różnych perspektyw. Każda technologia może wspierać monitoring innych obszarów IT, ale dopiero ich integracja pozwala zbudować pełniejszy obraz sytuacji bezpieczeństwa.

EDR (*ang. Endpoint Detection and Response*) – perspektywa punktu końcowego

- **Co robi:** monitoruje i analizuje zachowanie bezpośrednio na urządzeniach użytkowników oraz serwerach. Wykrywa anomalie w procesach, próby modyfikacji plików systemowych, podejrzane działania aplikacji oraz techniki wykorzystywane przez malware.
- **Główna funkcja:** izolowanie zainfekowanego urządzenia od sieci, blokowanie złośliwych procesów i ograniczanie skutków ataku na poziomie stacji roboczej lub serwera.

NDR (*ang. Network Detection and Response*) – perspektywa sieci

- **Co robi:** analizuje ruch sieciowy wewnątrz organizacji, w środowiskach lokalnych i chmurowych. Wykorzystuje analizę behawioralną, aby wykrywać nietypową komunikację, ruch boczny, próby eksfiltracji danych oraz połączenia z infrastrukturą atakujących.
- **Główna funkcja:** wykrywanie zagrożeń także tam, gdzie nie da się zainstalować agenta EDR, na przykład w systemach IoT (*ang. Internet of Things*), OT, urządzeniach sieciowych lub starszych systemach produkcyjnych.

XDR (*ang. Extended Detection and Response*) – szerszy kontekst incydentu

- **Co robi:** łączy dane z wielu warstw bezpieczeństwa, takich jak punkty sieciowe, sieć, chmura, poczta, aplikacje i tożsamość. Zamiast prezentować pojedyncze alerty
  z wielu narzędzi, pomaga zbudować jeden, spójny obraz ataku.
- **Główna funkcja:** korelacja zdarzeń, ograniczanie liczby odizolowanych alertów i szybsze wskazanie, które zdarzenia wymagają reakcji. XDR jest naturalnym krokiem w stronę platformizacji cyberbezpieczeństwa, bo łączy detekcję
  i reakcję w wielu obszarach środowiska IT.

SIEM (*ang. Security Information and Event Management*) – centralna warstwa analityczna

- **Co robi:** agreguje i analizuje logi z wielu źródeł, między innymi z systemów EDR, NDR, firewalli, baz danych, systemów tożsamości, aplikacji biznesowych i usług chmurowych.
- **Główna funkcja:** korelacja zdarzeń. SIEM łączy pojedyncze sygnały z różnych systemów w logiczny ciąg, co pozwala wykrywać ataki wieloetapowe i odróżniać zdarzenia krytyczne od szumu informacyjnego.

SOAR (*ang. Security Orchestration, Automation and Response*) – koordynacja reakcji

- **Co robi:** pobiera alerty, najczęściej z systemu SIEM lub XDR, i uruchamia zaprogramowane procedury reagowania, czyli playbooki.
  Łączy różne narzędzia bezpieczeństwa w jeden proces działania.
- **Główna funkcja:** automatyzacja powtarzalnych zadań, takich jak zablokowanie konta, odcięcie adresu IP, izolacja urządzenia, utworzenie zgłoszenia lub wysłanie powiadomienia do właściwego zespołu. Dzięki temu czas reakcji może zostać istotnie skrócony.

Cloud Security / CNAPP (*ang. Cloud-Native Application Protection Platform*) – perspektywa środowisk chmurowych

- **Co robi:** monitoruje konfigurację usług chmurowych, uprawnienia, workloady, kontenery, API oraz przepływy danych w środowiskach public cloud i hybrid cloud. Wykrywa błędne konfiguracje, nadmiarowe uprawnienia, podatne komponenty i podejrzane aktywności.
- **Główna funkcja:** ograniczanie ryzyka w chmurze oraz łączenie informacji o podatnościach, konfiguracji, tożsamościach i zachowaniu aplikacji z procesem detekcji oraz reakcji.

Od alertu do reakcji

Alert jest dopiero początkiem procesu. Samo wykrycie zdarzenia nie oznacza jeszcze, że organizacja jest bezpieczna. Kluczowe jest szybkie przejście od informacji o potencjalnym incydencie do decyzji i działań operacyjnych.

Dobrze zaprojektowany proces reagowania powinien obejmować kilka etapów:

- **Priorytetyzacja alertu:** ocena, czy zdarzenie jest krytyczne, jakich zasobów dotyczy i czy może oznaczać realny incydent.

- **Analiza kontekstu:** połączenie informacji z punktów końcowych, sieci, chmury, tożsamości, poczty i aplikacji, aby zrozumieć pełną ścieżkę ataku.
- **Ograniczenie skutków:** izolacja urządzenia, blokada konta, odcięcie komunikacji, wycofanie tokenów, zablokowanie podejrzanego procesu lub zatrzymanie dostępu do danych.
- **Usunięcie źródła incydentu:** eliminacja złośliwego oprogramowania, zamknięcie podatności, korekta błędnej konfiguracji lub zmiana reguł dostępu.
- **Przywrócenie bezpiecznego stanu:** weryfikacja, czy zagrożenie zostało zatrzymane, a systemy mogą wrócić do pracy bez ryzyka ponownej kompromitacji.
- **Wnioski po incydencie:** aktualizacja polityk, reguł detekcji, playbooków, procedur i konfiguracji narzędzi bezpieczeństwa.

W praktyce to właśnie ten ostatni etap decyduje o różnicy między pojedynczym incydentem a kryzysem operacyjnym. Im szybciej zespół bezpieczeństwa potrafi przejść od alertu do działania, tym mniejsze ryzyko przestoju, utraty danych, eskalacji uprawnień lub rozprzestrzenienia się ataku w organizacji.

SOC, czyli zespół, który zamienia alerty w reakcję

Do analizy, priorytetyzacji i przekładania alertów na konkretne działania niezbędne jest Security Operations Center (SOC). To wyspecjalizowane centrum operacyjne, które oddziela realne zagrożenia od fałszywych alarmów, ocenia ich ryzyko i natychmiast uruchamia procedury naprawcze (np. izolację urządzenia czy blokadę konta).

W przeciwieństwie do klasycznego działu IT, który dba o ciągłość działania i dostępność systemów, SOC koncentruje się wyłącznie na bezpieczeństwie. Posiadanie narzędzi takich jak SIEM czy EDR/XDR bez dojrzałego SOC-u sprawia, że organizacja widzi incydenty, ale nie potrafi na nie szybko i właściwie zareagować.

Budowa takiego zespołu to jednak ogromne wyzwanie logistyczne i kadrowe. Dlatego firmy mają do wyboru trzy drogi:

- **Wewnętrzny SOC:** własny zespół monitorujący sieć w trybie 24/7.
- **Zewnętrzny SOC (usługa MSP, *ang. Managed Service Provider*/MSSP, *ang. Managed Security Service Provider*):** pełne wsparcie zewnętrznych inżynierów i analityków, pozwalające uniknąć kosztów rekrutacji.
- **Model hybrydowy:** współpraca wewnętrznego działu IT z zewnętrznym zespołem ekspertów.

Niezależnie od wybranego modelu, to właśnie sprawnie działający SOC decyduje o tym, czy alert w systemie pozostanie tylko suchym komunikatem, czy stanie się początkiem skutecznej i natychmiastowej obrony.

Tożsamość jako nowy bastion cyberbezpieczeństwa

W nowoczesnych architekturach bezpieczeństwa coraz większe znaczenie ma ochrona tożsamości. Upowszechnienie pracy hybrydowej i zdalnej zwiększyło liczbę punktów dostępu do zasobów firmy, a aplikacje biznesowe zostały rozproszone między środowiska lokalne, rozwiązania SaaS, API i chmury obliczeniowe. Ponieważ sama sieć nie jest już zaufaną granicą, tożsamość użytkownika, urządzenia, aplikacji oraz usługi staje się jednym z głównych punktów kontroli.

Identity Centric Security wspiera model Zero Trust, w którym dostęp nie jest przyznawany domyślnie. Każda decyzja o jego przyznaniu jest wypadkową trzech elementów: tożsamości, kontekstu (uwzględniającego np. lokalizację, urządzenie, porę dnia, poziom ryzyka, zachowanie użytkownika) oraz sztywnej polityki bezpieczeństwa.

Aby skutecznie wykrywać i reagować na zagrożenia w tym obszarze, nowoczesny ekosystem bezpieczeństwa musi integrować wyspecjalizowane narzędzia ochrony tożsamości. Szczególne znaczenie mają technologie wspierające:

- **IAM (*ang. Identity and Access Management*) / IGA (*ang. Identity Governance and Administration*):** zarządzanie tożsamościami, uprawnieniami i cyklem życia dostępów użytkowników.
- **MFA (*ang. Multi-Factor Authentication*):** wieloskładnikowe uwierzytelnianie jako podstawowa bariera przed przejęciem konta.
- **PAM (*ang. Privileged Access Management*):** kontrola, monitorowanie i izolowanie kont uprzywilejowanych, które są jednym z najważniejszych celów atakujących.
- **ITDR (*ang. Identity Threat Detection and Response*):** wykrywanie i reagowanie na ataki wymierzone bezpośrednio w infrastrukturę tożsamości, na przykład Active Directory, Entra ID lub inne katalogi tożsamości.
- **Secrets Management:** ochrona sekretów, kluczy API, certyfikatów i poświadczeń wykorzystywanych przez aplikacje, automatyzacje, procesy DevOps oraz konta maszynowe.

Tożsamość jest dziś jednym z najważniejszych źródeł detekcji anomalii w dostępie do danych i systemów. Nietypowe logowanie, próba eskalacji uprawnień, użycie konta administracyjnego poza standardowym procesem, podejrzany dostęp do aplikacji SaaS lub masowe pobieranie danych mogą wskazywać na aktywny incydent.
Dlatego systemy ochrony tożsamości powinny być połączone z szerszym ekosystemem zapewniającym funkcje detekcji i reagowania.

Rola AI w detekcji, reakcji i nowych ryzykach

Sztuczna inteligencja (*ang. AI, Artificial Intelligence*) ma coraz większe znaczenie w wykrywaniu i reagowaniu na zagrożenia. Wspiera analizę dużych wolumenów danych, wykrywanie anomalii, korelację alertów, ocenę ryzyka oraz automatyczne rekomendowanie działań. Bez takich mechanizmów ręczna analiza miliardów zdarzeń dotyczących cyberbezpieczeństwa byłaby niewykonalna.

AI nie zastępuje jednak procesu bezpieczeństwa ani odpowiedzialności zespołu. Jest narzędziem, które może przyspieszyć analizę i ograniczyć szum informacyjny, ale wymaga dobrze zdefiniowanych źródeł danych, polityk, playbooków i kontroli jakości. W przeciwnym razie organizacja może szybciej przetwarzać alerty, ale nadal nie będzie wiedziała, które z nich mają realne znaczenie biznesowe.

Coraz więcej organizacji wdraża agenty AI, automatyzacje i narzędzia wspierające pracę z kodem, dokumentami lub danymi. Takie rozwiązania często wymagają dostępu do repozytoriów, baz danych, aplikacji biznesowych i sekretów technicznych. W praktyce stają się nową kategorią tożsamości maszynowych, które trzeba monitorować i kontrolować podobnie jak konta uprzywilejowane.

Z perspektywy procesu detekcji i reagowania oznacza to konieczność obserwowania nie tylko ludzi, ale również aplikacji, botów, kont serwisowych i agentów AI. Nietypowe pobieranie danych, zmiana zakresu uprawnień, dostęp do nowych repozytoriów lub użycie sekretów poza standardowym procesem powinny być traktowane jako sygnały ryzyka.

Rola kompetentnego zespołu w budowie architektury odporności

Technologia jest ważna, ale sama nie wystarczy. Organizacja może posiadać narzędzia EDR, NDR, XDR, SIEM, SOAR, PAM, ITDR i rozwiązania chmurowe, a mimo to nie mieć realnej zdolności do szybkiej reakcji. Kluczowe jest właściwe zaprojektowanie architektury, integracja systemów, tuning detekcji oraz dopasowanie procedur do rzeczywistego profilu ryzyka.

W osiągnięciu powyższego, przydatnym może okazać się współpraca z Trusted Advisorem – zaufanym doradcą, który posiada rzadką, ale głęboką i udokumentowaną kompetencję, i który skuteczne przeprowadzi firmę przez cały proces budowania odporności cyfrowej: od analizy środowiska, przez dobór architektury, po konfigurację, testy i optymalizację.

Taki zespół powinien wspierać organizację w kilku obszarach:

- **analiza obecnego środowiska:** identyfikacja narzędzi, luk, powielających się funkcji, ryzyk na styku systemów i obszarów bez wystarczającej widoczności;
- **dobór architektury:** określenie, które rozwiązania powinny pozostać, które trzeba zintegrować, a które warto zastąpić platformowym podejściem;
- **projektowanie scenariuszy detekcji:** przygotowanie reguł, przypadków użycia i korelacji odpowiadających realnym zagrożeniom dla danej organizacji;
- **automatyzacja reakcji:** budowa playbooków dla powtarzalnych zdarzeń, takich jak przejęcie konta, podejrzany ruch sieciowy, złośliwy plik, anomalia w chmurze lub eskalacja uprawnień;
- **testy i PoC (*ang. Proof of Concept*):** weryfikacja technologii w środowisku klienta, zanim stanie się elementem architektury bezpieczeństwa;
- **tuning i optymalizacja:** ograniczanie fałszywych alarmów, dopracowanie progów detekcji i dostosowanie konfiguracji do specyfiki organizacji;
- **wsparcie regulacyjne:** uwzględnienie wymagań NIS2, DORA i innych regulacji przy projektowaniu procesów wykrywania, raportowania i reakcji.

Jego celem powinno być zbudowanie architektury, która wykorzystuje istniejące inwestycje, eliminuje luki i daje zespołowi bezpieczeństwa realną zdolność do działania.

Podsumowanie

Wykrywanie i reagowanie na zagrożenia jest jednym z kluczowych elementów cyberodporności. Skuteczny model detekcji i reagowania wymaga widoczności w wielu warstwach środowiska, korelacji danych, automatyzacji reakcji, kontroli tożsamości oraz dobrze zaprojektowanej architektury.

Największą wartością nie jest jednak samo posiadanie narzędzi, ale ich właściwe połączenie z procesami i kompetencjami. Dopiero wtedy organizacja może szybciej przejść od alertu do decyzji, ograniczyć skutki incydentu i wzmacniać odporność na kolejne ataki.